Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB

Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Umsetzungsplan NCS

15. Mai 2013

Inhalt

1 Ausgangslage

Der Bundesrat hat am 27. Juni 2012 mit der Verabschiedung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)» den Grundstein für eine umfassende Behandlung der Cyber-Problematik gelegt. Die NCS fokussiert dabei auf die Frühwarnung vor Cyber-Risiken und auftauchenden Bedrohungen, eine allgemeine Stärkung der Widerstandsfähigkeit (Resilienz) der Schweizer Infrastrukturen und eine generelle Reduktion von Cyber-Risiken. Die Strategie enthält 16 konkrete Massnahmen, die in 7 Handlungsfelder eingeteilt sind. Diese müssen bis 2017 umgesetzt sein und in den regulären Betrieb überführt werden.

Die Handlungsfelder und ihre Massnahmen sind:

Handlungsfeld 1	**Massnahmen**	
Identifikation von Risiken durch Forschung	1	Neue Risiken im Zusammenhang mit der Cyber-Problematik sollen erforscht werden
Handlungsfeld 2	**Massnahmen**	
Risiko- und Verwundbarkeitsanalyse	2	Selbständige Überprüfung der Systeme Risikoanalysen zur Risikominimierung in Zusammenarbeit mit Behörden, den IKT-Leistungserbringern und Systemlieferanten
	3	IKT-Infrastruktur auf systemische, organisatorische, und technische Verwundbarkeiten untersuchen
Handlungsfeld 3	**Massnahmen**	
Analyse der Bedrohungslage	4	Erstellung Lagebild und Lageentwicklung
	5	Nachbearbeitung von Vorfällen für die Weiterentwicklung von Massnahmen
	6	Fallübersicht und Koordination interkantonaler Fallkomplexe
Handlungsfeld 4	**Massnahmen**	
Kompetenzbildung	7	Schaffung einer Übersicht über Kompetenzbildungsangebote und Identifikation von Lücken.
	8	Schliessung der Lücken bei Kompetenzbildungsangeboten und vermehrte Nutzung qualitativ hochstehender Angebote
Handlungsfeld 5	**Massnahmen**	
Internationale Beziehungen und Initiativen	9	Aktive Teilnahme der Schweiz im Bereich der Internet-Governance.
	10	Kooperation auf der Ebene der internationalen Sicherheitspolitik
	11	Koordination der Akteure bei der Beteiligung an Initiativen und Best-Practices im Bereich Sicherheits- und Sicherungsprozesse
Handlungsfeld 6	**Massnahmen**	
Kontinuitäts- und Krisenmanagement	12	Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen
	13	Koordination der Aktivitäten in erster Linie mit den direkt betroffenen Akteuren und Unterstützung der Entscheidfindungsprozesse mit fachlicher Expertise
	14	Aktive Massnahmen zur Identifikation der Täterschaft und allfälligen Beeinträchtigung deren Infrastruktur bei einer spezifischen Bedrohung
	15	Erarbeitung eines Konzeptes für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung
Handlungsfeld 7	**Massnahmen**	
Rechtsgrundlagen	16	Überprüfung bestehender Rechtsgrundlagen aufgrund der Massnahmen und Umsetzungskonzepte und Priorisierung von unverzüglichen Anpassungen

Die Grundannahme der Strategie ist, dass Cyber-Risiken eine Ausprägung bestehender Risiken in Prozessen und Strukturen darstellen. Cyber-Risiken entstehen durch den Einsatz von (vernetzten) IKT-Systemen, über die vermehrt alle Arten von Prozessen ausgeführt und betrieben werden. Sei dies das Versenden von Nachrichten über E-Mail anstelle eines Postbriefes oder die Bedienung hoch komplexer Steuerungs- und Produktionsanlagen über den Computer, anstelle einer manuellen Bedienung. Die Identifikation von Cyber-Risiken muss daher auf einer möglichst genauen Einschätzung der tatsächlichen Bedrohungslage für die einzelnen IKT-basierten Prozesse und deren Vernetzung aufbauen. Die zur Minimierung die-

ser Risiken erforderlichen Massnahmen dürfen sich jedoch nicht nur auf die IKT-Sicherheit konzentrieren. Massnahmen zur Minimierung von Cyber-Risiken müssen immer physische, personelle, technische sowie daraus resultierende organisatorische Dimensionen in Betracht ziehen und aufeinander abgestimmt werden. National kann dies nur durch die Wahrnehmung der Verantwortung jedes Einzelnen und eine Vernetzung der Massnahmen erfolgen.

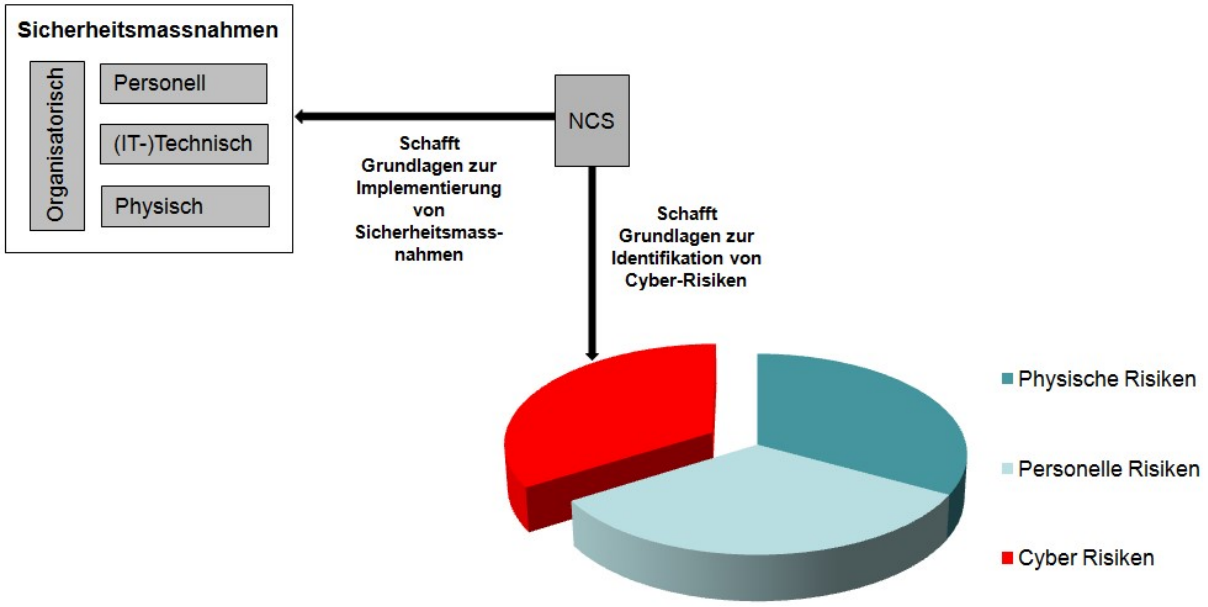

Abbildung 1: Cyber-Risiken und Sicherheitsmassnahmen

Die Umsetzung der Strategie soll koordiniert durch eine im EFD, genauer im Informatiksteuerungsorgan des Bundes (ISB), angesiedelte Koordinationsstelle erfolgen. Diese Koordinationsstelle (KS NCS) soll mit den verantwortlichen Stellen auf Stufe Bund und deren Partnern auf Stufe Kantone einen Umsetzungsplan der Strategie erarbeiten und dabei den allfälligen personellen Mehrbedarf der beteiligten Departemente und der Bundeskanzlei ab 2014 transparent und umfassend ausweisen.

Im Bereich des Schutzes der kritischen Infrastrukturen (KI) baut die Strategie auf der «Nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI-Strategie)» des Bundesamtes für Bevölkerungsschutz (BABS) auf. Die im Rahmen des SKI-Programms geplanten Risiko- und Verwundbarkeitsanalysen sollen auch Cyber-Risiken identifizieren und somit die Grundlage für eine einheitliche, branchenspezifische Risikominimierung schaffen. Die Risiko- und Verwundbarkeitsanalysen berücksichtigt die in der SKI-Strategie definierten Sektoren und Teilsektoren. An diesem Prozess sind die jeweils zuständigen Regulatoren und Aufsichtsbehörden beteiligt sowie das Bundesamt für Wirtschaftliche Landesversorgung (BWL) und das Bundesamt für Bevölkerungsschutz (BABS). Das BWL[1] und das BABS[2] sind bezüglich der ihnen zugewiesenen Teilsektoren zuständig für das Erstellen einer Risiko- und Verwundbarkeits-Analyse. Die Vorgehensweise und die Methoden sollen wo möglich und sinnvoll zwischen BWL und BABS abgesprochen werden. Es soll auch ein möglichst einheitlicher Ansatz verfolgt werden.

[1] Die 13 Teilsektoren des BWL sind: Energie (Erdgasversorgung, Erdölversorgung, Stromversorgung), Industrie (Chemie- und Heilmittelindustrie, Maschinen- Elektro- und Metallindustrie); Information und Kommunikation (Informationstechnologien, Telekommunikation); Nahrung (Lebensmittelversorgung, Wasserversorgung); Verkehr (Luftverkehr, Schienenverkehr, Schiffsverkehr, Strassenverkehr).

[2] Die 15 Teilsektoren des BABS sind: Behörden (Parlament, Justiz, Verwaltung; Forschung und Lehre, Kulturgüter, internationale Organisationen); Entsorgung (Abwasser, Abfallentsorgung); Finanzen (Banken, Versicherungen); Gesundheit (Ärztliche Betreuung und Spitäler, Labors); Information und Kommunikation (Medien, Postverkehr); Öffentliche Sicherheit (Armee, Blaulichtorganisationen, Zivilschutz).

Die Konsolidierung der Ergebnisse zu einer gesamtheitlichen Analyse der Bedrohungslage erfolgt in Zusammenarbeit mit der Melde-und Analyse Informationssicherung (MELANI).

Abhängigkeiten und Nahtstellen zur SKI-Strategie können wie folgt zusammengefasst werden:

- Die nationale SKI-Strategie gilt im Bereich der kritischen Infrastrukturen der Schweiz als Mantelstrategie. Die Strategie deckt den Schutz der kritischen Infrastrukturen vor Cyber-Risiken ab.
- Massnahmen in der NCS-Strategie, welche kritische Infrastrukturen betreffen, werden auf die Massnahmen der SKI-Strategie abgestimmt (z.B. Risiko- und Verwundbarkeitsanalysen).
- Die Umsetzung der Massnahmen der Strategie im Bereich der kritischen Infrastrukturen erfolgt in enger Koordination zwischen dem BWL, dem BABS und dem ISB.

Um die Massnahmen zu konkretisieren, hat die KS NCS in einem ersten Schritt Gespräche mit den involvierten Bundesämtern geführt (Interviewpartner siehe Anhang), Erkenntnisse gesammelt und konsolidiert. Dabei wurde der aktuelle Stand und die weitere Planung zur Umsetzung der Strategie erhoben. Folgende Erkenntnisse wurden ersichtlich:

a) Der Ansatz der Eigenverantwortung sowie die Subsidiarität des Bundes, wie er in der Strategie angestrebt wird, ist richtig.
b) Nach Durchführung der geplanten Risiko- und Verwundbarkeitsanalysen können auf Grund übergeordneter, nationaler Interessen, Handlungsbedarf und Mehrkosten zur Behebung bestehender Risiken anfallen.
c) Einige Departemente haben im Rahmen ihrer Aufgaben bereits Vorarbeiten zur Umsetzung von Massnahmen geleistet.
d) Es ist ein klarer Ressourcenbedarf auszuweisen.

Der vorliegende Umsetzungsplan des EFD stellt die Grundlage für die Departemente und Ämter dar, um die betreffenden Massnahmen zu konkretisieren und zu implementieren. Er macht keine konkreten Aussagen über die genauen Aufgaben und Pflichten der zu schaffenden Stellen, dies obliegt den jeweiligen Organisation, basierend auf den Erfahrungen auf Grund ihres Tagesgeschäftes. Ausgangspunkt sind die in der Strategie festgelegten Massnahmen, die bis Ende 2017 umzusetzen und in den regulären Betrieb zu überführen sind.

Die Kantone werden über den Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) in diesen Umsetzungsprozess eingebunden. Ausserdem soll die KS NCS in Zusammenarbeit mit dem KKM SVS eine «Fachgruppe Cyber» unterstützen, in welcher Bund, Kantone und Gemeinden vertreten sind.

Die NCS schliesst den Kriegs- und Konfliktfall explizit aus. Die Armee ist für den Schutz und die Abwehr von Gefahren für die eigenen Infrastrukturen und Systeme in allen Lagen selbstverantwortlich. Zusätzlich soll sie in ihrem Auftrags- und Verantwortungsspektrum auch Lösungsansätze für die Behandlung der Cyber-Bedrohungen und ihrer Konsequenzen bestimmen. Der Chef der Armee hat dazu einen Delegierten Cyber-Defence der Armee ernannt, welcher seine Arbeit am 1. Januar 2013 aufgenommen hat.

2 Auftrag und Rahmenbedingungen

Weil die angestrebte Erhöhung der Sicherheit im Umfeld der Cyber-Risiken nur durch ein Zusammenwirken der Verwaltung, der kantonalen Behörden, der Sektoren/Teilsektoren sowie der Betreiber kritischer Infrastrukturen erreicht werden kann, bindet die Strategie alle diese Akteure in die Massnahmenumsetzung ein.

Der Umsetzungsplan wurde mit starkem Einbezug des Bundesamtes für Wirtschaftliche Landesversorgung (BWL) und des Bundesamtes für Bevölkerungsschutz (BABS) erstellt. Auch der Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS), der die Schnittstelle von Bund und Kantonen ist, wurde als zentraler Umsetzungspartner einbezogen.

3 Gewonnene Erkenntnisse

3.1 Ressourcenbedarf

Die Bedarfsschätzungen wurden in den Interviews konsolidiert und basieren auf bereits bestehenden Bedarfsausweisen und Positionspapieren der relevanten Ämter in diesem Bereich oder leiten sich aus den Massnahmen in der vorliegenden Strategie ab. Weil die Wahrnehmung der Cyber-Ausprägung der bereits bestehenden Prozesse der Bundesverwaltung zur Umsetzung der NCS-Massnahmen mit einer Mehrbelastung einher geht, besteht ein Ressourcenbedarf.

Vertieftes Expertenwissen zu ähnlichen Themen im Cyber-Bereich ist in verschiedenen Ämtern gefragt. Um dieses Wissen gemeinsam aufzubauen und auch weiterzugeben wurden geeignete Zusammenarbeitsformen diskutiert. So beispielsweise für den regulatorischen Bereich, in dem sich Synergien für Fachbehörden wie das Bundesamt für Zivilluftfahrt (BAZL), dem Bundesamt für Strassen (ASTRA), das Bundesamt für Energie (BFE) u.a. ergeben werden. Hier besteht Bedarf, z.B. Fragestellungen zu Cyber-Risiken durch den zunehmenden Einsatz von Steuerungs- und Kontrollsystemen gemeinsam zu erörtern. Auch eine punktuelle Mitwirkung bei Inspektionen, sofern Cyber-spezifische Bereiche betroffen sind, könnten durch die gleichen Personen ausgeführt werden. Inwiefern die Departemente diesen Bedarf über einen Expertenpool abdecken könnten, welcher spezialisierte, fachlich deckungsgleiche Ressourcen bei einer Stelle konzentriert und den Fachämtern zur Verfügung stellt, ist noch offen und wird geprüft.

Die Strategie hat den Grundauftrag von MELANI (VBS und EFD) dahingehend erweitert, dass die Stelle im Rahmen der Umsetzungsarbeiten verpflichtet wird, zusätzliche Leistungen im Bereich Lagebild, Unterstützung und Nachbearbeitung von Vorfällen und Unterstützung bei Risiko- und Verwundbarkeitsanalysen bei den KI-Betreibern wahrzunehmen. Weiter sollen IKT-Leistungserbringer und Systemlieferanten stärker von MELANI einbezogen werden. MELANI erfüllt damit eine zentrale Rolle bei der Umsetzung der Strategiemassnahmen, indem die Stelle die Koordination, Auswertung und Weiterleitung des Informationsflusses im Zusammenhang mit der Bewältigung von Cyber-Risiken übernimmt und den Informationsaustausch mit den KI-Betreibern, den relevanten IKT-Leistungserbringern und den Systemlieferanten sicherstellt. Diese auszubauende Informations-Drehscheibe bildet das Herzstück der Strategie. Nach Abschluss der Umsetzungsarbeiten Ende 2017 soll MELANI, wo nötig, eine Koordinations- und Leitfunktion innerhalb ihres Auftrages übernehmen. MELANI-Aufgaben werden daher in der untenstehenden Tabelle gesondert ausgewiesen.

Departemente	neue Stellen	Abbau bis Ende 2017	Umsetzung folgender Massnahmen NCS
EDA	+2	0	7;8;9;10;11;13
EJPD	+1	-1	4;6;13;14
VBS	+17	0	2;3;4;5;6;11;12;13;14
EFD	+6	-1	2;3;4;5;6;7;8;9;10;11;12;13;14;16
WBF	+2	0	2;12;13
UVEK	+2	0	2;3;7;8;9;10;11;12
Total	+30	-2	
MELANI (Ressourcen bereits ausgewiesen unter EFD + VBS)	+6	0	2;3;4;5;6;10;11;12;13;14

3.2 Relevanz der Sektoren, Teilsektoren und KI-Betreiber

Der Bund allein kann die Nationale Cyber-Resilienz nur beschränkt durch eigene Massnahmen stärken. Die ausgewiesenen Aufwände des Bundes dienen dazu, die optimalen Rahmenbedingungen für eine gestärkte Nationale Cyber-Resilienz zu schaffen. Die Mitarbeit der kritischen Sektoren und Teilsektoren der Wirtschaft und die entsprechenden Betreiber kritischer Infrastrukturen sind ein wichtiger Teil der Umsetzung der Strategie-Massnahmen. Deshalb ist deren erfolgreiche Einbindung in die entsprechenden Massnahmen durch die zuständigen Bundesämter mittels geeigneter Informations- und Konsultationsprozesse notwendig. Anhaltspunkte für die Kompetenzteilung sind in der SKI-Strategie zu finden.

3.3 Subsidiarität der Armee

Obwohl die NCS explizit den Kriegs- und Konfliktfall ausklammert und der Armee den Auftrag gibt, sich für diese Spezialfälle vorzubereiten, verfügt die Armee über wesentliches Wissen vor allem in technischen Belangen im Bereich der Cyber-Risiken. Diese vorhandenen Fähigkeiten sollten von den verantwortlichen Ämtern in ihren Umsetzungsprozessen bei Bedarf eingebaut und abgerufen werden können. Dies entspricht dem bewährten Ansatz der Subsidiarität des Einsatzes der Armee z. B. bei Naturkatastrophen. So soll in einem ersten Schritt in den für die Umsetzung der NCS verantwortlichen Ämtern und Verwaltungsbereichen das Wissen und die Fähigkeiten im Umgang mit Cyber-Risiken auf- oder ausgebaut werden, die ein lösungsorientiertes und zielführendes Abrufen der Fähigkeiten und des Wissens der Armee erlauben. Eine frühe Koordination mit der Umsetzung NCS heisst somit, dass Synergien in diesen Bereichen von den verantwortlichen Ämtern identifiziert und genutzt werden könnten. Eine frühe Einbindung soll somit auch dazu führen, das von der Armee zu erarbeitende Cyber-Defense Konzept auf das Gesamtsystem Schweiz abzustimmen.

3.4 Projektrisiken Umsetzung NCS

Es gibt einige Risiken, die bei der Umsetzung der Strategie zu berücksichtigen sind. Eines der mit Abstand grössten Risiken ist, dass die Umsetzungsmassnahmen nicht rechtzeitig greifen. Andere sind:

- Risiken, die aufgrund von fehlendem Wissen bei den einzelnen Akteuren entstehen, sowie das Eintreten von Zwischenfällen, bei welchen die Umsetzung der Strategie zu spät kommt und diese dadurch in den Augen der Öffentlichkeit obsolet macht.
- Der Einbezug der Sektoren und Teilsektoren sowie der KI-Betreiber durch die Ämter erfolgt zu spät oder ungenügend, was die Risiko- und Verwundbarkeitsanalyse sowie das Kontinuitätsmanagement gefährden könnte.
- Die Kooperation ist durch ungenügende Kommunikation und falsche Erwartungen auf Seiten der Sektoren, Teilsektoren und der KI-Betreiber gefährdet.
- Durch die nicht zeitgerechte Aufstockung der benötigten Ressourcen ist die Umsetzung der Massnahmen in allen Bereichen der Strategie gefährdet.
- Infolge der Umsetzung der Strategie könnte hinsichtlich einiger kritischer Infrastrukturen Handlungsbedarf ersichtlich werden, was wiederum heisst, dass zur Behandlung der entsprechenden Risiken gewisse Kosten anfallen könnten.

4 Umsetzungsorganisation NCS

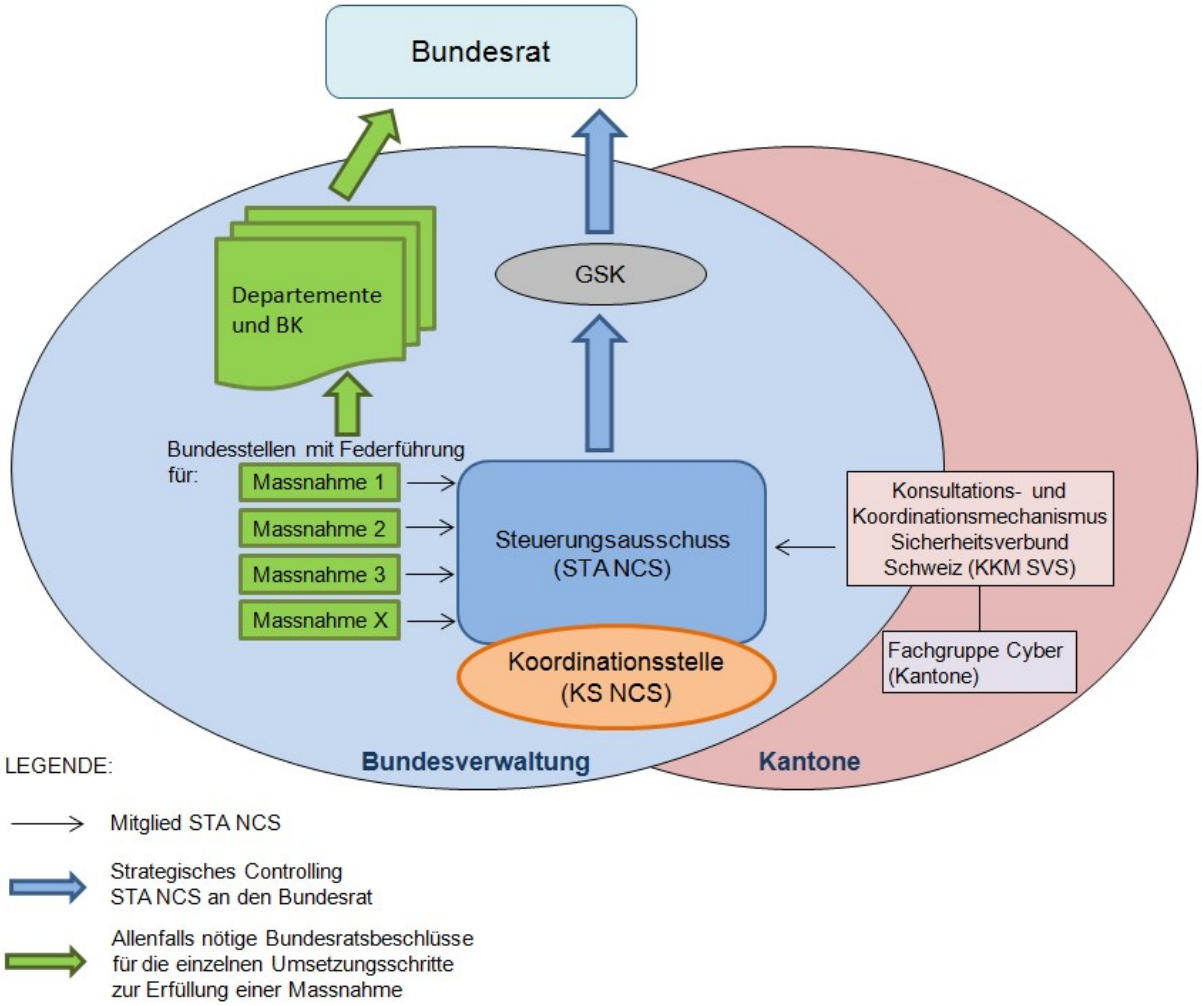

Abbildung 2: Umsetzungsorganisation NCS

4.1 Steuerungsausschuss NCS

Der Steuerungsausschuss NCS stellt im Auftrag des Bundesrates die koordinierte, zielgerichtete Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» sicher (siehe Abbildung 2).

Er hat folgende Kompetenzen und Funktionen:

- Er überprüft durch ein strategisches Controlling den zielorientierten und terminlichen Fortschritt des Massnahmenportfolios der Strategie und rapportiert diesen via GSK an den Bundesrat.
- Er sorgt für ein koordiniertes Vorgehen der zuständigen Departemente bei der Umsetzung der Massnahmen, insbesondere wenn diese den Rechtsetzungsbereich tangieren.
- Er unterstützt aktiv die Zusammenarbeit der Bundesstellen mit den relevanten Stellen aus Kantonen, Wirtschaft und Zivilgesellschaft.

- Er stellt sicher, dass bei den Umsetzungsaktivitäten eine Berücksichtigung der Risikopolitik des Bundes, der «Nationalen Strategie zum Schutz kritischer Infrastrukturen» und der «Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz» erfolgt.
- Er überprüft mit den verantwortlichen Stellen mögliche Synergien sowie eine Vereinfachung und Verschlankung der Meldewege und –systeme.
- Er verfolgt die Entwicklungen der Cyber-Risiken und unterbreitet dem Bundesrat diesbezügliche Empfehlungen für die Weiterentwicklung der Strategie.
- Er erstattet dem Bundesrat via Eidgenössisches Finanzdepartement (EFD) jährlich Bericht zum Stand der Strategieumsetzung, Ende 2017 in Form eines umfassenden Schlussberichts mit einer Wirksamkeitsüberprüfung der Strategie und ihres Umsetzungsplanes. Die Wirksamkeitsüberprüfung wird dem Bundesrat bereits im Frühjahr 2017 vorgelegt.

Im Steuerungsausschuss vertreten sind alle Departemente mit federführender Verantwortung für zumindest eine der Umsetzungs-Massnahmen. Ebenfalls im Steuerungsausschuss vertreten ist der Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS). Den Vorsitz führt das EFD.

4.2 Koordinationsstelle NCS

Die Koordinationsstelle NCS koordiniert die Umsetzung der Strategie auf operationeller und fachlicher Ebene.

Sie hat folgende Aufgaben:

- Sie beobachtet und bewertet systematisch den Fortschritt der Strategie-Umsetzungsarbeiten und informiert den Steuerungsausschuss.
- Sie koordiniert und unterstützt die Umsetzungsaktivitäten der verantwortlichen Stellen und führt ihr zugeordnete Massnahmen durch.
- Sie erkennt und nutzt Synergien zwischen den Umsetzungsmassnahmen.
- Sie organisiert die Zusammenarbeit mit bundesinternen und –externen Expertinnen und Experten, wie auch mit deren Organisationen.
- Sie verfolgt national und, in Absprache mit dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA), international die Entwicklungen in Sachen Cyber-Strategien und deren Umsetzung und kommuniziert die Erkenntnisse zeitnah den relevanten Umsetzungspartnern.
- Sie führt jährlich eine Expertenveranstaltung NCS durch, an welcher sich die Umsetzungspartner schweizweit vernetzen, informieren und austauschen können.

4.3 Fachgruppe Cyber (FG-C) und Fachgruppe International (FG-CI)

Um die Arbeiten mit Schnittstellen zu den Kantonen zu koordinieren, konstituiert der Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz (KKM SVS) die Fachgruppe Cyber (FG-C) bestehend aus Vertretern der Stufen Bund, Kantone und Gemeinden.

Die Fachgruppe Cyber (FG-C) koordiniert die NCS-Umsetzung auf Stufe Kanton. Sie hat folgende Aufgaben:

- Sie bezieht die Kantone als die zentralen Partner des Bundes in sämtliche sie betreffenden Umsetzungsmassnahmen ein.
- Sie leitet Teilprojekte in der Form von Arbeitsgruppen in den Bereichen «Resilienzstärkung», «Incident Handling» und «Krisenmanagement».
- Sie koordiniert die Umsetzung der kantonalen Teilprojekte und überprüft durch strategisches Controlling die zielorientierten und termingerechten Fortschritte.
- Sie stellt den umfassenden Wissensstand der Fachgruppe über die Umsetzungstätigkeiten des Bundes im Rahmen der Strategie sicher und fördert den Erfahrungsaustausch zwischen den Mitgliedern der Fachgruppe.

Die Koordinationsstelle NCS ist Mitglied der Fachgruppe Cyber des KKM SVS und bildet auf Stufe Bund die Brücke mit den Projektarbeiten der Fachgruppe Cyber, um Synergien optimal zu nutzen und Redundanzen zu vermeiden.

Weiter ist eine Fachgruppe Cyber International (FG-CI), unter der Federführung des EDA geplant. Ziel dieser FG-CI ist es, den Informationsfluss in enger Kooperation/Koordination zwischen allen Beteiligten sicher zu stellen. Das EDA wird Parteien, welche sich für die internationale Zusammenarbeit im Cyber-Bereich interessieren, zu einer konstituierenden Sitzung einladen. Anlässlich dieses ersten Treffens soll diskutiert werden, wie eine interdepartementale Arbeitsgruppe, welche sich ausschliesslich mit den internationalen Aspekten der Thematik befasst, für die Teilnehmenden hilfreich sein kann.

5 Massnahmen und Verantwortlichkeiten

Die sieben Handlungsfelder mit den jeweiligen Strategie-Massnahmen (M1-M16) können entsprechend ihrer zeitlichen Entfaltung und Abhängigkeiten in folgende vier Bereiche zusammengefasst werden:

- **Massnahmen im Bereich der Prävention**
- **Massnahmen im Bereich der Reaktion**
- **Massnahmen im Bereich des Kontinuitäts- und Krisenmanagements**
- **Massnahmen im Bereich Unterstützende Prozesse**

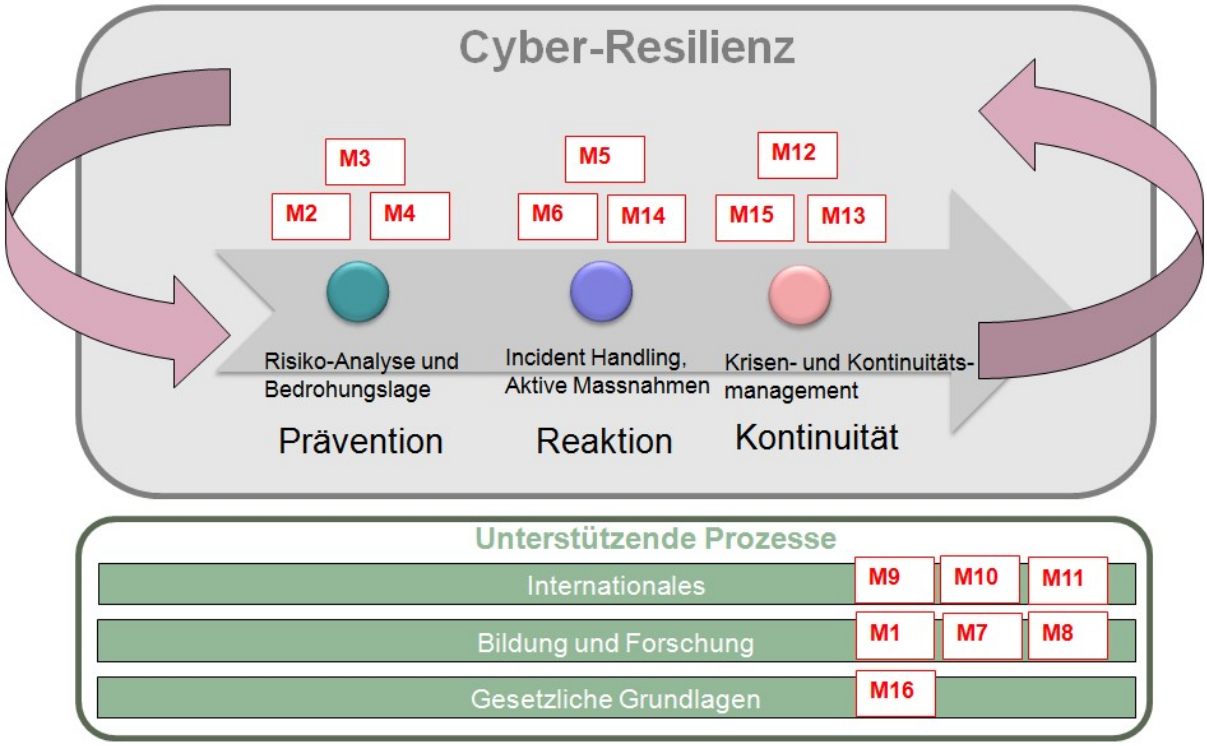

Abbildung 3: Die Strategie auf einen Blick

Die Cyber-Resilienz besteht aus wiederkehrenden Prozessen der Prävention, Reaktion und Kontinuität. Nach dem Krisenmanagement in einem Ereignisfall beginnt der Prozess jeweils wieder von vorne.

Im nächsten Kapitel werden die Erkenntnisse der Gespräche mit den Interviewpartnern erläutert, gegliedert nach Bereichen und Massnahmen sowie deren Verantwortlichkeiten, Zuständigkeiten, Umsetzungsziele und Liefertermine.

5.1 Massnahmen im Bereich der Prävention

Im Bereich der Prävention soll der Ansatz des Gesamtrisikomanagements aus der SKI-Strategie auch für das Cyber-Risiko im Sinne der Strategie zur Anwendung kommen. Die für die Umsetzung verantwortlichen Ämter veranlassen das Erstellen einer Risiko- und Verwundbarkeitsanalyse. Dies geschieht in erster Linie federführend durch das BWL und die jeweils zuständigen Fachbehörden und Regulatoren.

Im Bereich der Darstellung der gesamtheitlichen Bedrohungslage ist die Zusammenführung von technischen und nicht-technischen Informationen notwendig, um Cyber-Risiken umfassend zu analysieren und zu bewerten. Diese Informationen werden von MELANI zur Verfügung gestellt. MELANI soll deshalb als zentrale Informations-Drehscheibe für die Kantone und die KI-Betreiber ausgebaut werden.

Es darf angenommen werden, dass die meisten kritischen Sektoren sowie Teilsektoren und die entsprechenden Betreiber kritischer Infrastrukturen eine Risiko- und Verwundbarkeitsanalyse institutionalisiert haben. Aufgrund der wachsenden Bedrohung muss mit der Strategie erreicht werden, dass der Cyber-Aspekt in der Gesamtrisikoanalyse explizit berücksichtigt wird. Die Strategie empfiehlt, dafür einen einheitlichen Ansatz zu verfolgen und die konsolidierten Ergebnisse als Lagedarstellung mit Lageentwicklungsmöglichkeiten zusammenzufassen.

Mit diesem Ansatz soll auch gewährleistet werden, dass Cyber-Risiken speziell bei KI-Betreibern transparent ausgewiesen werden. Somit können, auf Grund übergeordneter und nationaler Überlegungen, inakzeptable Restrisiken erfasst und anfallende Kosten für den identifizierten Handlungsbedarf nachvollziehbar dargelegt werden.

Handlungsfeld 2	**Zuständigkeiten: BWL, BABS, Fachbehörden/Regulatoren;** MELANI	**Massnahme 2**
Risiko- und Verwundbarkeitsanalyse	Das BWL erarbeitet zusammen mit den Sektoren, Teilsektoren und den KI-Betreibern die Risiko- und Verwundbarkeits-Analysen. Sektoren und Teilsektoren, die nicht durch das BWL erfasst werden, sind durch das BABS, unter Einbezug der zuständigen Fachbehörden, anzugehen. Es gibt eine klare Zuständigkeit zwischen BWL und BABS für Teilsektor-Verantwortlichkeiten.	Selbstständige Überprüfung der Systeme. Risikoanalysen zur Risikominimierung in Zusammenarbeit mit Behörden, den IKT-Leistungserbringern und Systemlieferanten.

Umsetzung:

Das BWL[3] und das BABS[4] sind für die ihnen zugewiesenen Teilsektoren jeweils zuständig für das Erstellen einer Risiko- und Verwundbarkeits-Analyse. Die Vorgehensweise und die Methoden sollen wo möglich und sinnvoll zwischen BWL und BABS abgesprochen werden. Sektoren und Teilsektoren, die nicht durch das BWL erfasst werden sind durch das BABS unter Einbezug der entsprechenden Fachbehörden (verantwortliche Regulatoren) anzugehen. Es soll auch ein möglichst einheitlicher Ansatz erfolgen. Die Arbeiten sollen bis Ende 2017 abgeschlossen werden.

Die Konsolidierung der Ergebnisse zu einer gesamtheitlichen Analyse der Bedrohungslage erfolgt in Zusammenarbeit mit MELANI.

[3] Siehe FN 1
[4] Siehe FN 2

Handlungsfeld 2	**Zuständigkeiten: ISB;** BIT, FUB, MELANI	**Massnahme 3**
Risiko- und Verwundbarkeitsanalyse	Das ISB erstellt zusammen mit den IKT-Leistungserbringern ein Prüfkonzept. Dieses kann als Ergänzung zum SKI-Leitfaden im Cyber-Bereich dienen. MELANI stellt den Austausch mit den KI-Betreibern, IKT-Leistungserbringern und Systemlieferanten sicher.	Die IKT-Infrastruktur soll auf systemische, organisatorische, und technische Verwundbarkeiten untersucht werden: Die Behörden, KI-Betreiber und Forschungseinrichtungen untersuchen ihre IKT-Infrastrukturen unter Einbezug der IKT-Leistungserbringer und Systemlieferanten auf Verwundbarkeiten.

Umsetzung:

Der Sicherheitsbereich im ISB (ISB-SEC) erstellt bis Ende 2015 ein Prüfkonzept, welches von den zuständigen Leistungserbringern und den jeweiligen Verantwortlichen in den Generalsekretariaten der Departemente umgesetzt wird. Das Bundesamt für Informatik und Telekommunikation (BIT) und die Führungsunterstützungsbasis (FUB) unterstützen als IKT-Leistungserbringer dieses Prüfkonzept. Dieses Prüfkonzept kann als Empfehlung der Wirtschaft und den KI Betreiber abgegeben werden. Das Prüfkonzept kann zudem durch die Fachgruppe Cyber des KKM SVS den Kantonen vorgestellt werden und somit als Empfehlung und Unterstützung der eigenen Überprüfung dienen.

Das Prüfkonzept wird mit laufenden Projekten koordiniert, wie z.B. das Information Security Management Systems (ISMS)von der Informations-und Objektsicherheit (IOS).

Die Konsolidierung der Ergebnisse zu einer gesamtheitlichen Analyse der Bedrohungslage erfolgt in Zusammenarbeit mit MELANI.

Handlungsfeld 3	**Zuständigkeiten: MELANI, NDB, KOBIK;** FUB, MND, BIT	**Massnahme 4**
Analyse der Bedrohungslage	Aus öffentlichen und nicht öffentlichen Quellen werden nachrichtendienstliche, polizeiliche, forensische und technische Informationen zur Bedrohungs- und Risikolage im Cyber-Bereich beschafft. Diese Massnahme wird in verschiedenen Vorhaben mit jeweils unterschiedlichen federführenden Stellen umgesetzt. MELANI generiert in enger Zusammenarbeit mit dem NDB und fedpol/KOBIK ein Bild der aktuellen Bedrohungslage. Der Nachrichtendienst (NDB) deckt die Cyber-Ausprägung seines Auftrages ab. CERTs: Aufbau der technischen Kapazitäten zur konstanten Überwachung (24/7): CSIRT-BIT, NDB-CSIRT, GovCERT.	Erstellung Lagebild und Lageentwicklung.

Umsetzung:

MELANI: Erstellung (bis Ende 2013) und Umsetzung (ab 2014) eines Konzeptes zur Stärkung von MELANI als Plattform für den Informationsaustausch. MELANI baut die systematische Zusammenarbeit mit relevanten IKT-Leistungserbringern und Systemlieferanten aus. Verstärkter Informationsaustausch mit den KI-Betreibern und der Wirtschaft.

NDB: Aufbau von Spezialwissen und Fähigkeiten im Cyber-Bereich beim NDB, mit FUB-ZEO und dem militärischen Nachrichtendienst (MND) als Leistungserbringer für den NDB (2014-2015).

Die technischen Kapazitäten zur konstanten Überwachung (24/7) der Bundesnetze sind per Ende 2015 aufzubauen.

- CERTs: MELANI: Ausbau GovCERT zur Erhöhung der Durchhaltefähigkeit (2014-2016)
- BIT: Ausbau des CSIRT um die Detektionsfähigkeit zu erhöhen

5.2 Massnahmen im Bereich der Reaktion

Die für das «incident handling» und «incident response» relevanten NCS-Massnahmen dienen zur Stärkung bestehender Aufgaben und Kapazitäten, welche zur Cyber-Resilienz beitragen und nicht durch einzelne Akteure wahrgenommen werden können. Im Laufe des «incident handling» und «incident response» kann unter Umständen auch die Notwendigkeit für gezielte, aktive Gegenmassnahmen entstehen. Wie weit die Schweiz hier fähig sein soll, unterhalb der Kriegsschwelle im Ausland aktive Massnahmen zu ergreifen, ist abschliessend im politischen Entscheidprozess festzulegen.

Handlungsfeld 3	**Zuständigkeiten: MELANI, NDB;** FUB, MND, BIT	**Massnahme 5**
Analyse der Bedrohungslage	Der Bund, Kantone und KI-Betreiber sollen relevante Vorfälle nachbereiten und Möglichkeiten zur Weiterentwicklung der eigenen Massnahmen im Umgang mit Vorfällen im Zusammenhang mit Cyber-Risiken überprüfen. MELANI sammelt, bewertet und analysiert die Erkenntnisse und stellt sie den relevanten Akteuren zur Verfügung (PPP Model). Auftrag NDB, wie in M4.	Nachbearbeitung von Vorfällen für die Weiterentwicklung von Massnahmen.
Umsetzung: Wie in M4 BIT: Aufbau der technischen Fähigkeiten (Steigerung der Reaktionsmöglichkeit auf einen Incident) zu einer 24/7-Überwachung. Bis 2014 soll der Ausbau des CSIRT-BIT zur Stärkung der technischen Kapazität und der Durchhaltefähigkeit erfolgen. Mit diesem Ausbau kann M4 unterstützt werden.		

Handlungsfeld 3	**Zuständigkeiten: KOBIK;** MELANI	**Massnahme 6**
Analyse der Bedrohungslage	Unmittelbare Verantwortung für die Strafverfolgung bei Cyber Vorfällen liegt bei den Kantonen**.**	Fallübersicht und Koordination interkantonaler Fallkomplexe.

Umsetzung:

Fedpol erarbeitet unter Einbezug der Kantone ein Konzept zur Führung einer gesamtheitlichen Fallübersicht (Straffälle) und zur Koordination von interkantonalen Fallkomplexen. Das Konzept geht durch zwei Vernehmlassungen in den Kantonen und wird durch die Konferenz der Kantonalen Justiz- und Polizeidirektoren (KKJPD) genehmigt. Innerhalb von fedpol übernimmt KOBIK die Koordination. Das Konzept soll bereits bestehenden Projekten zwischen Kantonen und Bund spezielle Beachtung schenken (beispielsweise Harmonisierung der Polizeiinformatik HPI; Informationsplattform „PICAR“ zur Schaffung einer Fallübersicht im Bereich Einbruchskriminalität). Im zweiten Quartal 2013 soll eine Kerngruppe der Projektorganisation definiert werden. Diese besteht aus Vertretern der:

Fedpol, KKJPD, Konferenz der Strafverfolgungsbehörden der Schweiz (KSBS), Konferenz der Kantonalen Polizeikommandanten der Schweiz (KKPKS), Leiter AG IT der KKPKS, Vertreter Swiss Police ICT, ein Vertreter der Bundesanwaltschaft (BA) und des Bundesamtes für Justiz (BJ) definiert werden.

Die erste Vernehmlassungen findet im zweiten Quartal 2014 und die zweite im vierten Quartal 2014 statt. Das Konzept soll bis zum dritten Quartal 2015 erstellt und durch die KKJPD gutgeheissen werden. Im vierten Quartal 2015 erfolgt dann die Ämterkonsultation. Die Vorbereitung der Realisierung folgt im Jahr 2016.

Auf internationaler Ebene sind Europol sowie Interpol massgebliche Akteure, mit denen das Konzept abgestimmt werden muss.

Die gewonnenen Informationen aus der Fallübersicht (Straffälle) und Erkenntnisse zu Fallkomplexen aus der technisch-operativen Analyse der Strafverfolgung fliessen über MELANI in die gesamtheitliche Analyse der Bedrohungslage ein.

Handlungsfeld 6	**Zuständigkeiten: NDB, MELANI;** KOBIK, MND	**Massnahme 14**
Kontinuitäts- und Krisenmanagement	Der NDB ist grundsätzlich dafür verantwortlich, mit nachrichtendienstlichen Mitteln Informationen zu beschaffen, diese zu analysieren und auszuwerten, um anschliessend die Resultate verbreiten zu können. Er baut unter Einbezug der FUB als technischem Leistungserbringer und dem MND als Verbindung zu den militärischen Nachrichtendiensten die Fähigkeiten zur Durchführung der Identifikation der Täterschaft auf und bereitet im Falle der politischen Opportunität entsprechende aktive Massnahmen vor. Zudem spielt KOBIK (fedpol) eine wichtige Rolle bei der Strafverfolgung und Identifikation der Täterschaft. KOBIK wird entsprechend einbezogen.	Aktive Massnahmen zur Identifikation der Täterschaft. Wenn dem NDB die Identifikation der Täterschaft gelingt, übergibt er, soweit rechtlich zulässig, die entsprechenden Informationen an die Bundesanwaltschaft. Diese entscheidet, ob sie ein Strafverfahren einleitet. Sollte keine Strafverfolgung angezeigt oder möglich sein, sind aktive Gegenmassnahmen vorzubereiten. Die entsprechende Rechtsgrundlage ist im NDG vorzusehen.

Umsetzung:

Anpassung des SLA (Service Level Agreement) mit FUB-ZEO bis Ende 2013. Aufbau von Spezialwissen bei NDB mit FUB-ZEO und MND als Leistungserbringer für den NDB (2014-2015).

Die Erkenntnisse der Analyse der Bedrohungslage durch MELANI und die im Rahmen des gesetzlichen Auftrages der Strafverfolgung liegenden Möglichkeiten zur Ermittlung und Überführung der Täterschaft fliessen in die Massnahmen ein.

5.3 Massnahmen im Bereich des Kontinuitäts- und Krisenmanagements

Vom Staat wird erwartet, dass er über Mittel verfügt, die es ihm ermöglichen, verantwortliche Stellen subsidiär zu unterstützen, wenn diese nicht mehr fähig sind, Massnahmen zu deren Bewältigung selber zu ergreifen. MELANI mit seinen Zulieferanten (insbesondere NDB) leistet eine solche Unterstützung im Rahmen des GK (Geschlossener Kundenkreis von MELANI). Diese Leistungen sind in allen Sektoren, Teilsektoren und bei den Betreibern kritischer Infrastrukturen zu verankern.

Die Prozesse für die Incident-Analyse und das Kontinuitäts- und Krisenmanagement müssen eng miteinander abgestimmt sein. Eine Krise wird in der Regel durch einen Incident ausgelöst. Nicht jeder Incident wächst sich jedoch zu einer Krise aus. Es braucht demnach Eskalationsprozesse vom «incident handling» zum Krisenmanagement. Pläne für das Krisenmanagement sind Teil des Kontinuitätsmanagements. Es ist deshalb Sache der zuständigen Ämter, sowie zuständigen Fachbehörden und Regulatoren, für ihren Verantwortungsbereich dafür zu sorgen, dass die Sektoren sowie Teilsektoren und entsprechenden Betreiber kritischer Infrastrukturen über ein funktionierendes «incident handing» und Krisenmanagement verfügen.

Handlungsfeld 6	**Zuständigkeiten: BWL, BABS, Fachbehörden/ Regulatoren;** MELANI	**Massnahme 12**
Kontinuitäts- und Krisenmanagement	Im Bereich Kontinuitätsmanagement sind die Zuständigkeiten wie bei M2.	Stärkung und Verbesserung der Widerstandsfähigkeit (Resilienz) gegenüber Störungen und Ereignissen.
Umsetzung: Die Umsetzung des Kontinuitätsmanagement ist wie in M2. Dazu passt das WBF im Rahmen der Revision des Landesversorgungsgesetz (LVG) seine Kompetenzen an. Das Kontinuitätsmanagement ist ein laufender Prozess. Es setzt auf den vorhandenen Risiko- und Verwundbarkeitsanalysen auf und kann demnach erst durchgeführt werden, wenn M2 abgeschlossen ist. MELANI unterstützt und stärkt den freiwilligen Informationsaustausch mit KI-Betreibern, IKT-Leistungserbringern und Systemlieferanten untereinander zur Unterstützung der Kontinuität und Widerstandsfähigkeit auf der Basis der Selbsthilfe. Dies führt zu einem erhöhten Bedarf an forensischen Fähigkeiten und zu einem zunehmenden Informationsfluss.		

Handlungsfeld 6	**Zuständigkeiten: BWL, MELANI, BABS;** KOBIK, EDA, Fachbehörden/Regulatoren	**Massnahme 13**
Kontinuitäts- und Krisenmanagement	Im Bereich Krisenmanagement sind die Zuständigkeiten wie bei M2 und M12. MELANI übernimmt den operativen Teil und stellt in einer Krise die subsidiäre Unterstützung der betroffenen Akteure mit der Bereitstellung von Expertenwissen sicher. Um die Strafverfolgung sicherstellen zu können, wird fedpol/KOBIK eng mit einbezogen. Bei Fällen mit möglichen aussenpolitischen Implikationen ist das EDA möglichst rasch zu informieren und bei der Erarbeitung von entsprechenden Vorsorgeplanungen einzubinden. Die federführenden Ämter koordinieren und stimmen sich untereinander ab.	Koordination der Aktivitäten in erster Linie mit den direkt betroffenen Akteuren und Unterstützung der Entscheidfindungsprozesse mit fachlicher Expertise.

Umsetzung:

Die Umsetzung des Krisenmanagements ist wie in M12. Dazu beantragt das WBF im Rahmen der Revision des LVG eine Anpassung seiner Kompetenzen. Das Krisenmanagement ist ein kontinuierlicher Prozess. Es setzt auf den vorhandenen Risikoanalysen auf und kann demnach erst durchgeführt werden, wenn diese abgeschlossen ist.

Mit MELANI und deren Partnern im Geschlossenen Kundenkreis (GK) bestehen funktionierende Prozesse, um eskalierende Incidents mit den existierenden Krisenorganisationen in der Verwaltung und der Wirtschaft zu behandeln.

Um ein einheitliches und vergleichbares Vorgehen gewährleisten zu können und die etablierten Kontakte gut zu nützen, ist ein koordiniertes Vorgehen zwischen BWL und BABS wichtig.

Handlungsfeld 6	Zuständigkeit: BK	Massnahme 15
Kontinuitäts- und Krisenmanagement	Unter der Federführung der Bundeskanzlei (BK) soll ein Konzept für Führungsabläufe- und Prozesse zur zeitgerechten Problemlösung erstellt werden, das auch den Cyber-Ausprägungen gerecht wird.	Erarbeitung eines Konzeptes für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung.
Umsetzung: Das (allgemeine) Krisenmanagement muss angepasst werden und auch den Cyber-Aspekt beinhalten. Führungsabläufe und -prozesse des Bundes tragen innerhalb bestehender Prozesse der Cyber-Ausprägung Rechnung. Unter Federführung der BK soll ein Konzept für Führungsabläufe und -prozesse zur zeitgerechten Problemlösung erstellt werden, das auch den Cyber-Ausprägungen gerecht wird.		

5.4 Unterstützende Prozesse

Da der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken im nationalen Interesse der Schweiz liegt, sind auch die dafür notwendigen Grundlagen zu schaffen. Dazu gehören:

- die Überprüfung, ob die bestehenden Rechtsgrundlagen den Schutzmassnahmen gerecht werden,
- die internationalen Kooperationen und Bemühungen, den Cyber-Raum mit international vereinbarten Regeln und Standards vor Missbrauch zu schützen,
- der Austausch von Erfahrungen, Forschungs- und Entwicklungsarbeiten, vorfallbezogenen Informationen sowie Ausbildungs- und Übungstätigkeiten,
- das Mitwirken der Schweiz im Rahmen von internationalen staatlichen und nichtstaatlichen Organisationen zur Minderung von Cyber-Risiken.

Um die Cyber-Resilienz erhöhen zu können, müssen die Fähigkeiten vorhanden sein, Risiken im Zusammenhang mit der Cyber-Problematik in der eigenen Verantwortungsdomäne zu identifizieren, zu bewerten und zu analysieren. Dazu sind durch die Strategie die zuständigen Bundesämter mit der Umsetzung der unten folgenden Massnahmen beauftragt worden, welche sie teilweise in Zusammenarbeit mit den zuständigen Stellen der Kantone angehen. Kantone und KI-Betreiber müssen sich zur Stärkung der Cyber-Resilienz auf diese Grundlagen abstützen können, da es sich um Staatsaufgaben handelt, die nicht durch die einzelnen Akteure wahrgenommen werden können.

Handlungsfeld 1	Zuständigkeiten: Verantwortliche Bundesstellen	Massnahme 1
Identifikation von Risiken durch Forschung	Werden im Verlauf der weiteren Umsetzungen konkretisiert.	Neue Risiken in Zusammenhang mit der Cyber-Problematik sollen erforscht werden.

Umsetzung:

Folgende Ansprechgruppen können Wissens- und Fähigkeitslücken im Cyber-Bereich identifizieren:

- CERTs
- KI-Betreiber
- IKT-Anbieter

Folgende Stellen führen Cyber-Research Projekte/Programme:

- EU
- ETH Abteilungen
- Universitäten und Fachhochschulen
- IKT Forschungslabs (z. B. IBM)

Handlungsfeld 4	Zuständigkeiten: KS NCS; BAKOM, EDA, BSV	Massnahme 7
Kompetenzbildung	Die Koordinationsstelle NCS erstellt in Zusammenarbeit mit dem BSV (Programm Jugend und Medien)[5], EDA und BAKOM eine Übersicht der Kompetenzbildungsangebote. Die Erarbeitung der Übersicht erfolgt in Abstimmung mit den Umsetzungsarbeiten der «Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz» und den Kantonen. Das EDA vermittelt Informationen über Angebote im Rahmen von internationalen Organisationen und Institutionen.	Schaffung einer Übersicht über Kompetenzbildungsangebote.

Umsetzung:

Die Übersicht über bestehende Kompetenzbildungsangebote soll bis Ende 2013 erstellt werden und Kompetenzbildungsangebote bis Mitte 2014 veröffentlicht werden.

[5] BRB 11.06.2010, Nationales Programm Jugendmedienschutz und Medienkompetenzen.

Handlungsfeld 4	**Zuständigkeiten: KS NCS;** BAKOM, EDA, BSV	**Massnahme 8**
Kompetenzbildung	Die Koordinationsstelle NCS koordiniert in Abstimmung mit der «Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz», den Kantonen und der Wirtschaft und in Zusammenarbeit mit dem BSV, EDA BAKOM und betroffene Fachbehörden und Regulatoren, die Erarbeitung eines Umsetzungskonzepts zur vermehrten Nutzung von bestehenden qualitativ hochstehenden Angeboten zum Umgang mit Cyber-Risiken und zur Schaffung von neuen formellen und informellen Kompetenzbildungsangeboten. Das EDA vermittelt Informationen über Angebote im Rahmen von internationalen Organisationen und Institutionen.	Schliessung der Lücken bei Kompetenzbildungsangeboten und vermehrte Nutzung von Angeboten.
Umsetzung: Ein Umsetzungskonzept zur vermehrten Nutzung von bestehenden Angeboten zum Umgang mit Cyber-Risiken sowie neue Kompetenzbildungsangebote sollen bis Ende 2015 geschaffen werden.		

Handlungsfeld 5	**Zuständigkeiten: BAKOM;** Fachbehörden/Regulatoren, EDA, SIPOL, MELANI	**Massnahme 9**
Internationale Beziehungen und Initiativen	Unterstützung vom UVEK, EDA, VBS und EFD. Das BAKOM nimmt aktiv an den relevanten internationalen Prozessen und Institutionen im Bereich Internet Governance (insbesondere ICANN, ITU, CSTD und IGF) teil, identifiziert fortlaufend die für die Stabilität, Verfügbarkeit und Sicherheit des Internets relevanten Aspekte, koordiniert die Schweizer Interessen mit Vertretern aus Verwaltung, Wirtschaft und Zivilgesellschaft und vertritt diese Interessen in den genannten Prozessen und Institutionen.	Internet Governance: Die Schweiz setzt sich aktiv und soweit möglich koordiniert für eine Internet-Governance ein, welche mit den Schweizer Vorstellungen von Freiheit und (Selbst-)Verantwortung, Grundversorgung, Chancengleichheit, Menschenrechten und Rechtsstaatlichkeit vereinbar ist.
Umsetzung: Das BAKOM und EDA, unter Einbezug des VBS in Sicherheitspolitischen Fragen (GS-VBS/SIPOL), erarbeiten per Ende 2013 in Zusammenarbeit mit den beteiligten Departementen, eine Übersicht zu den prioritären Veranstaltungen, Initiativen und internationalen Gremien mit Bezug zur Internet-Governance. Weiter nimmt das BAKOM kontinuierlich aktiv an den relevanten Aktivitäten im Bereich Internet Governance teil.		

Handlungsfeld 5	**Zuständigkeiten: EDA;** SIPOL, MELANI, BAKOM	**Massnahme 10**
Internationale Beziehungen und Initiativen	Das EDA soll in internationaler Zusammenarbeit gezielte Aktivitäten in Gang setzen. Eine denkbare Möglichkeit ist die Etablierung eines «Code of Conduct» im Zusammenhang mit dem Aspekt Cyber. Langfristiges Ziel ist es, völkerrechtlich verbindliche Richtlinien festzulegen. Zudem wird die Idee verfolgt, Genf als Standort für Internet-Fragen zu etablieren/auszubauen. Das EDA wird für die Umsetzung dieser Massnahme durch das GS-VBS/SIPOL unterstützt.	Kooperation auf der Ebene der internationalen Sicherheitspolitik, um der Bedrohung im Cyber Raum in Zusammenarbeit mit anderen Staaten und internationalen Organisationen zu begegnen. Es sollen in internationaler Zusammenarbeit gezielte Aktivitäten in Gang gesetzt, respektive fortgeführt werden, damit die Schweiz ihre Interessen in den verschiedenen internationalen Gremien wahren kann.
Umsetzung: Ein EDA-internes, mittelfristiges Konzept zur NCS-Umsetzung in internationaler Zusammenarbeit soll bis Ende 2013 erstellt werden. MELANI und BAKOM unterstützen diesen Prozess.		

Handlungsfeld 5	**Zuständigkeiten: KS NCS;** Fachbehörden/Regulatoren, EDA, MELANI	**Massnahme 11**
Internationale Beziehungen und Initiativen	MELANI und die Fachbehörden sowie Regulatoren stärken den Informationsaustausch unter den KI-Betreibern, den IKT-Leistungserbringern und Systemlieferanten zu internationalen Ansätzen und Initiativen. Damit unterstützen MELANI und UVEK die koordinierte Einbringung des Wirtschaftstandortes Schweiz in diesen internationalen Gremien. Sofern gewünscht, stellen MELANI, UVEK und EFD in Absprache mit den Departementen, insbesondere dem EDA die Teilnahme sicher.	Koordination der Akteure bei der Beteiligung an Initiativen und Best Practices im Bereich Sicherheits- und Sicherungsprozesse. Im Rahmen privater und staatlicher Initiativen, Konferenzen und Standardisierungsprozesse im Bereich Sicherheit und Sicherung koordinieren sich die Betreiber, Verbände und Behörden, um sich in diese Gremien einzubringen.
Umsetzung: In einem ersten Schritt sollen die beteiligten Partner (Fachbehörden und Regulatoren) eine Bestandesaufnahme machen, wer grundsätzlich bei internationalen Initiativen und Gremien dabei sein soll. In einem zweiten Schritt soll eine Konsolidierung erfolgen. Dazu werden Fachbehörden, Industrie und gegebenenfalls das EDA einbezogen. Die KS NCS koordiniert diesen Prozess.		

Handlungsfeld 7	**Zuständigkeiten: KS NCS**	**Massnahme 16**
Rechtsgrundlagen	Die Koordinationsstelle NCS des ISB koordiniert die Arbeiten zur Massnahme 16 mit den zuständigen Departementen. Für die als prioritär identifizierten Gesetzgebungslücken und nötigen rechtlichen Anpassungen erarbeiten die zuständigen Departemente die nötigen Entwürfe auf den passenden Normstufen.	Überprüfung bestehender Rechtsgrundlagen.
Umsetzung: Die Koordinationsstelle NCS erarbeitet per Ende 2013 zusammen mit den Departementen eine erste Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarfs im Cyber-Bereich. Für die als prioritär identifizierten Gesetzgebungslücken ist dem Bundesrat bis spätestens Ende 2014 ein Regelungskonzept mit Zeitplanung zu unterbreiten.		

6 Anhang

Referenzierte Dokumente

Titel	Autor/ Herausgeber	Datum
[1] Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken	VBS	19.06.2012
[2] Nationale Strategie zum Schutz kritischer Infrastrukturen	VBS – BABS	27.06.2012
[3] Leitfaden Schutz Kritischer Infrastrukturen	VBS – BABS	Entwurf 23.07.2012
[4] Handbuch Risikomanagement Bund	EFD	Version 1.0

Liste der Interviewpartner

Bundesstellen	Teilnehmer	Datum
BWL-BABS-ISB (Abstimmungssitzung)	Ruedi Rytz (BWL), Toni Lauber (BWL), Stefan Brem (BABS), Nick Wenger (BABS), Pascal Lamia (ISB), Stefanie Frey (ISB), Franz Zingg (ISB), Marc Henauer (NDB)	07.01.2013
BAKOM	Armin Blum	17.01.2013
BAV	Petra Breuer, Ulrich Schär, Heinz Geiser	14.01.2013
BAZL	Urs Haldimann	11.01.2013
BFE	Christian Holzner, Hans-Peter Binder	17.01.2013
BIT	Heino Kronenberg	17.01.2013
BSV	Thomas Vollmer	27.02.1013
EDA	Michele Coduri, Christoph Bühler	21.01.2013
fedpol-KOBIK	Roland Becker, Thomas Walther, Tobias Bolliger	11.01.2013
FINMA	Marc Sander	04.01.2013
FUB	Riccardo Sibilia, Gérald Vernez	11.01.2013
GS-VBS	Jürg Treichler	14.01.2013
ISB-MELANI	Pascal Lamia, Stefanie Frey	18.01.2013
ISB-SEC	Marcel Frauenknecht, Franz Zingg, Daniel Graf	11.01.2013
KKM SVS	Bernhard Wigger, Dario Walder	14.01.2013
NDB	Philipp Kronig, Reto Camenisch	17.01.2013

Abkürzungen

Abkürzung	Beschreibung
Betreiber KI	Betreiber Kritische Infrastrukturen
BFT	Bildung Forschung und Technologie
BIT	Bundesamt für Informatik und Telekommunikation im Eidg. Finanzedpartement
BVS	Bundesamt für Sozialversicherungen
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
GK	Geschlossener Kundenkreis (Element von MELANI)
FG-C	Fachgruppen Cyber
FUB	Führungsunterstützungsbasis des VBS
FUB-ZEO	Zentrum für Elektronische Operationen in der Führungsunterstützungsbasis des VBS
GSK	Konferenz der Generalsekretäre
ISB-SEC	Sektion Informatiksicherheit im Informatiksteuerungsorgan des Bundes
KKJPD	Konferenz der kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KKPKS	Konferenz der Kantonalen Polizeikommandanten der Schweiz
KSBS	Konferenz der Strafverfolgungsbehörden der Schweiz
KKM SVS	Konsultations- und Koordinationsmechanismus Sicherheitsverbund Schweiz
KOBIK	Koordinationsstelle zur Bekämpfung der Internetkriminalität im EJPD
KS NCS	Koordinationsstelle zur Umsetzung der Strategie
LVG	Bundesgesetz vom 8. Oktober 1982 über die wirtschaftliche Landesversorgung (Landesversorgungsgesetz, LVG)
MELANI	Melde- und Analysestelle Informationssicherung
MND	Militärischer Nachrichtendienst im VBS
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
SiLAN NDB	Sicherheits-LAN des NDB
SIPOL	Sicherheitspolitik (Organisationseinheit beim GS-VBS)
SKI Strategie	Nationalen Strategie zum Schutz Kritischer Infrastrukturen
SONIA	Sonderstab Information Assurance
STA NCS	Steuerungsausschuss Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken